Network Security *28 Credit Hours*

After reviewing attack vectors and network diagrams, this class provides a further look at network protocols and the OSI and Internet Models. Building on this knowledge, topics such as firewalls, intrusion detection, and security event monitoring are covered to relate and emphasize the necessity for proper device management. At the end of the course the gained knowledge will be used to assess weaknesses in controls during a live pen test lab and demonstration in a simulated banking environment.

July 17-12, 2017

Operating Systems *28 Credit Hours*

This course focuses on the security capabilities and limitations of network and computer Operating Systems ("OSs"). Systems reviewed include virtualization, the Microsoft OS family (including Windows Server, Clients and desktop management), the UNIX/Linux operating system family, IBM's OS/400 and mobile OSs. Hands-on exercises use virtualized or native environments, and activities include the review and application of a foundational risk framework across the various OSs to better understand risks from an abstract perspective.

September 11-15, 2017

STREAM
Supervision Technology Risks
Educate, Analyze and Manage

Last updated: 01/20/17

IT Topics	Examiner IT Bootcamp	Mobile & e-Banking	IS Vuln. Mgt.	Net Sec	OS
Mobile Banking Technologies and Payments	✓	✓			
Mobile Devices		✓			✓
E-Banking Technologies		✓			
Common Threats and Vulnerabilities	✓	✓	✓		
Cyber Security		✓	✓	✓	
Strong Authentication and Multi-Layer Security (SR 11-9)		✓			
Managing Mobile Banking and E-Banking Risks		✓			
Vendor Management	✓	✓			
Change and Patch Management	✓		✓		✓
Microsoft Security Tools			✓		
Penetration Testing	✓		✓	✓	
Vulnerablility Testing		✓	✓		
Intrusion Detection/ Prevention	✓		✓	✓	
Incident Response			✓		
Firewall Architecture				✓	
Network Diagramming	✓			✓	
TCP/IP Protocol	✓			✓	
Wireless				✓	
Active Directory	✓				✓
Microsoft OS s	✓				✓
Unix/Linux OS					✓
IBM OS/400					✓
Network OS					✓
Virtualization	✓		✓		✓
BYOD (Bring Your Own Device)	✓	✓			
Cloud Computing	✓				
Data Leak Prevention	✓				
Social Media and Risks	✓				
Cyber Insurance			✓		
"Internet of Things"				✓	

How to Register

Federal Reserve and State* Examiners
Contact your Reserve Bank training coordinator

U.S. Federal Regulators*
Contact: **Samantha Kolep**
Federal Reserve of Chicago
(312) 322-5507
STREAM@chi.frb.org

Non–U.S. Regulators
Contact: **Maribeth Seraj**
International Training and Assistance
Federal Reserve Board of Governors
(202) 736-5557
BSRInternationalTraining@frb.gov

Registration Questions?
For any other Registration Questions
Contact: **Samantha Kolep**
(312) 322-5507
STREAM@chi.frb.org

***A nonrefundable registration fee of $550.00 will apply to all non-Federal Reserve System State and Agency participants.**

STREAM
Supervision Technology Risks
Educate, Analyze and Manage

The STREAM Technology Lab is focused on maintaining, developing and delivering interactive, hands-on educational opportunities and support services along with risk-based analytical tools. Key activities of the team include educating examiners, peers and stakeholders on the risks associated with existing and emerging technologies with a focus on understanding both the tactical examination perspective and the strategic implications associated with managing those risks.

Federal Reserve Bank of Chicago
230 South LaSalle Street
Chicago, IL 60604

Onsite Contact: **Steven Langford**
(312) 322-5768
Steven.Langford@chi.frb.org

Technology Lab

2017 Course Schedule

STREAM
Supervision Technology Risks
Educate, Analyze and Manage

Course Offerings

The underlying premise of the STREAM Technology Lab is to address the critical knowledge gaps between Examiners and industry IT practitioners created by the increasing complexity of Information Technology and Security, and their impact on Operational Risk. We strive to offer a rich, innovative learning environment that combines classroom lecture with "hands-on" labs and interactive exercises to help Examiners narrow those gaps and better understand risks in today's banking environment.

What's New for 2017

- **New content:** Based on feedback from participants and instructors we review and update our courses, and consider recent themes such as ransomware, account take-over/key loggers and financial technologies with respect to the underlying IT concepts along with examiner relevance.
- **New labs:** We continually look for opportunities to introduce and enhance hands-on labs and other interactive exercises. The topic of cybersecurity threats is covered in various IT classes through hands-on exercises, demonstrations and interactive exercises that incorporate foundational and applied network and security concepts to promote an understanding of risks and controls.

Banking Applications Classes

ALM Model Lab *28 Credit Hours*

In addition to asset-liability management theory and exam considerations, this course offers hands-on ALM model training to commissioned examiners responsible for ALM model reviews at community, regional and large banking organizations. Topics include ALM model mechanics and assumption development, stochastic simulation and valuation techniques, rate term structure modeling, prepayment models, deposit modeling, and dynamic liquidity modeling. Note: Class registration is limited and completion of prerequisites may apply. Contact Amir Moaiery at 312-322-5197 directly for any questions.
Recommended Audience: Course material is advanced; registrants are expected to have a solid understanding of financial concepts and have exam responsibilities for reviewing ALM models.

May 22-26, 2017 ; July 31-August 4, 2017 ; November 13-17, 2017

BSA/AML Hands-On Lab *28 Credit Hours*

This entry level course is designed to walk examiners through core principles and basic procedures of the FFIEC BSA Anti-Money Laundering Examination Manual. Topics include: Examination Scoping and Planning; Risk Assessments; Customer Identification Program/ Customer Due Diligence; Currency Transaction Reports, Office of Foreign Asset Control; Information Sharing; Suspicious Activity Monitoring & Reporting; and, Developing conclusions and finalizing the examination.
Recommended Audience: Safety & Soundness examiners (pre- and post-commissioned) who are expected to perform BSA exams. Registrants should have participated on at least one BSA exam.

June 5-9, 2017 ; September 18-22, 2017

Bank Operations Simulation *32 Credit Hours*

This course provides participants with a simulated bank operations experience. Utilizing an industry-standard general ledger system and related applications, participants receive hands-on training on fundamental banking operations, including cash, teller and check operations, back office operations, investment and loan operations and electronic payments systems (ACH, Wire Transfer, Remote Deposit Capture and more.) Participants experience the bank management perspective to manage bank operations, detect misappropriations, and work to mitigate control weaknesses. The participants also improve their understanding of examiner responsibilities by identifying issues and root causes that contribute to control weaknesses.
Recommended Audience: Safety & Soundness examiners (especially pre-commissioned) who are looking for bank operations training. Federal Reserve registrants should have participated on at least one review of community bank operations. The class is also open to Reserve Bank personnel in other departments who are looking for greater understanding of bank general ledger accounting and operations.

July 10-14, 2017 ; October 16-20, 2017

Payments Systems and Risks *24.75 Credit Hours*

This course provides an in depth examination of the core payments systems in existence today: Automatic Clearing House (ACH); checks and image-based checks; debit and credit cards; wires; mobile banking; and, wholesale payment systems. The participants can gain a thorough knowledge of the characteristics and uses of each payments system, participant roles and responsibilities, the operational aspects of the payment methods, and the potential risks associated with the core payments systems along with the rules and laws governing compliance. The course also covers emerging trends in fraud and fraud prevention, the data security and privacy and evolving risks in the alternative payments.
Recommended Audience: Safety & Soundness examiners who are expected to perform payment exams as part of operational risk or credit risk focus areas.

July 24-28, 2017 ; October 30-November 3, 2017

Information Technology Classes

IT Generalist Courses

Recommended Audience: The following courses are recommended for newer IT examiners and for Safety & Soundness examiners who are being cross-trained to do IT exams.

Examiner IT Bootcamp *28 Credit Hours*

The "Examiner IT Bootcamp Hands-On" course is a foundational course designed for safety and soundness and other examiners who are exposed to IT-related issues during examinations and who have a basic understanding or interests in IT concepts, supervision, and risks for financial institutions. The course presents and builds on foundational concepts including IT audit, risk frameworks, networks and operating systems, and covers applied topics of risks including system management, controls, data management, and emerging technologies. The course includes interactive discussions, multimedia presentations, instructor demonstrations and participant hands-on labs.

June 12-16, 2017 ; September 25-29, 2017

e-Banking/Mobile Banking *28 Credit Hours*

This course provides participants with an overview of the technologies and risks fundamental to electronic and mobile banking. Topics include technology overview, common security threats and vulnerabilities, fraud risks, virtual currencies, vendor management sound practices. Evolving trends and risks around mobile banking applications, Bring Your Own Device (BYOD) and mobile OSes are also covered. Hands-on exercises include vulnerability testing, SQL injection compromise, account takeover fraud, and vendor due diligence. Mitigating controls such as web application testing and the FFIEC's strong authentication guidance are also covered.

June 19-23, 2017

Information Security Vulnerability Management *28 Credit Hours*

This course focuses on the operational aspects of information security vulnerability management. Topics include network and system monitoring, risk assessment and mitigation, patch management, and incident response. Hands-on exercises with penetration testing, vulnerability scanning and patch management tools reinforce the necessity for bank IT managers to have an accurate asset inventory and risk assessment.

May 15-19, 2017 ; October 23-27, 2017

IT Risk Specialist Courses

Recommended Audience: The following two courses are recommended for IT risk specialist examiners of all experience levels who are looking to deepen their technical knowledge or be updated on the latest issues.

Continued on back page